MRA 構成

MRA 構成の概要

この章には、互換性のあるエンドポイントにモバイルおよびリモートアクセスを提供する基本構成を完了する方法を説明する構成タスクが含まれています。これらの手順は、単一クラスタ、複数クラスタ、単一ドメイン、および複数ドメインのシナリオに使用できます。

MRA 設定タスクフロー

次のタスクを完了し、モバイルおよびリモートアクセスの基本設定を完了します。

始める前に

- MRA を構成する前に、MRA 要件の章を確認してください。
- MRA を展開するために必要な証明書がシステムにあることを確認してください。詳細については、証明書の要件を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Expressway サーバーアドレスの設定 （3 ページ）	Expressway-C および E サーバーごとに、システムのホスト名、ドメイン名、および NTP ソースを設定します。
ステップ 2	SIP の有効化 （3 ページ）	Expressway-E と Expressway-C の両方で SIP が有効になっていることを確認します。

	コマンドまたはアクション	目的
ステップ 3	自動侵入保護の構成 （4 ページ）	推奨。Expressway-C で自動侵入保護を無効にし、Expressway-E で有効にします。
ステップ 4	モバイルおよびリモートアクセスを有効にする （4 ページ）	Unified Communications モードをモバイルおよびリモートアクセスに設定します。
ステップ 5	ドメインの追加 （5 ページ）	Expressway-C で、内部 UC ドメインと、エッジドメインやプレゼンスドメインなどの他の関連ドメインを追加します。
ステップ 6	内部 UC クラスタの追加 • Unified CM クラスタの追加 • IM and Presence Service クラスタの追加 • Cisco Unity Connection クラスタの追加	各 Expressway-C クラスタから、内部 UC クラスタへの接続を作成します。
ステップ 7	MRA アクセス制御の構成 （10 ページ）	OAuth 認証や SAML SSO 設定など、MRA アクセス制御の設定を構成します。
ステップ 8	UC アプリケーションで OAuth を構成する （20 ページ）	推奨。システムがサポートしている場合は、OAuth 認証を構成します。
ステップ 9	SAML SSO の設定 （22 ページ）	オプション。SAML SSO を設定して、外部 Jabber クライアントとユーザーの Unified CM プロファイル間で共通アイデンティティを許可します。
ステップ 10	セキュアトラバーサルゾーンの構成 （27 ページ）	Expressway-C と Expressway-E の間に暗号化された UC トラバーサルゾーンを設定します。

次のタスク

基本的な MRA セットアップを完了したら、次の章を参照してください。

- ICE メディアパスの最適化—ICE は、MRA コールのメディアパスを最適化するオプション機能です。ICE により、MRA に登録されたエンドポイントは、メディアが WAN および Expressway サーバーをバイパスするように、メディアを相互に直接送信できます。
- 機能と追加構成— MRA 機能とオプションの構成については、この章を参照してください。
- MRA デバイスの導入準備— システムを構成した後、デバイスアクティベーションコードは、リモート MRA デバイスの導入準備をするための安全な方法を提供します。

Expressway サーバーアドレスの設定

この手順を使用して、Cisco Expressway-C および Expressway-E サーバーのそれぞれに FQDN と NTP サーバーを設定します。

（注） エッジドメインが複数ある場合でも、1つの Expressway サーバーは、1 つのホスト名とドメイン名を保持できます。

ステップ 1 Cisco Expressway-C で、サーバーアドレス情報を設定します。

a) **[システム（System）]** > **[ドメインネームシステム（DNS）（DNS）]**の順に選択します。
b) このサーバーに、**システムホスト名**と**ドメイン名**を割り当てます。
c) ドメインを検出する際に Expressway がクエリする 最大 5 台の ドメインネームシステム（DNS）サーバーに IP アドレスを入力します。これらのフィールドには FQDN ではなく、IP アドレスを使用する必要があります。

（注） 分割ドメインネームシステム（DNS）を展開する場合は、Expressway-C は内部サーバーを指し、Expressway-E は、パブリックドメインネームシステム（DNS）サーバーを指します。

ステップ 2 [NTP 設定の構成（Configure NTP Settings）] :

a) **[システム（System）]** > **[時刻（Time）]**メニューの順に選択し、信頼できる NTP サーバーを指します。
b) NTP 認証方式を入力する方法

- 無効 ー 認証が使用されていません
- Symmetric キーーこのメソッドを使用する際は、キー ID、ハッシュメソッドおよび Pass フレーズを指定する必要があります。
- 秘密キー—自動生成された秘密キーを使用します。

ステップ 3 Expressway-C クラスタにある各サーバーにこの手順を繰り返します。

ステップ 4 Expressway-C を設定したら、Expressway-E クラスタ内の各サーバに対してこの手順を繰り返します。

SIP の有効化

Expressway-C および Expressway-E クラスタで SIP を有効にします。

（注） SIP および H.323 プロトコルは、X8.9.2 以降のバージョンの新しいインストールで、デフォルトで無効になっています。

ステップ 1 Expressway-C プライマリピアで、**[構成（Configuration）]** > **[プロトコル（Protocols）]** > **[SIP]**の順に選択します。

ステップ 2 **[SIPモード（SIP mode）]** を**オン**にします。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Expressway-E プライマリピアでこの手順を繰り返します。

自動侵入保護の構成

Expressway-C で自動侵入保護を無効にし、Expressway-E でサービスを有効にすることをお勧めします。

（注） Expressway-C が X8.9 以降で新しくインストールされた場合、自動侵入保護サービスはデフォルトで Expressway-C と Expressway-E の両方で実行されます（これをチェックします）。

ステップ 1 Expressway-C で、自動侵入保護を無効にします。

a) **[システム（System）]** > **[管理（Administration）]**の順に選択します。
b) **[自動保護サービス（Automated protection service）]** を **[オフ（Off）]** にします。
c) [保存（Save）] をクリックします。

ステップ 2 Expressway-E で、自動侵入保護を有効にします（サービスはデフォルトでオンになっています）。

a) **[システム（System）]** > **[管理（Administration）]**の順に選択します。
b) **[自動保護サービス（Automated protection service）]** を **[オン（On）]** に設定します。
c) **[保存（Save）]** をクリックします。

（注） 同じ IP アドレスを使用する複数の MRA ユーザーがいる場合（たとえば、同じパブリック IP アドレスを持つ NAT の背後に複数の MRA ユーザーがいる場合）、同じ IP アドレスからのすべてのトラフィックが原因で、自動侵入保護がトリガーされる可能性があります。この場合、IP アドレスに除外を設定します。詳細については、「例外の設定」を参照してください。

モバイルおよびリモートアクセスを有効にする

ドメインとトラバーサルゾーンを構成設定する前に、Expressway でモバイルおよびリモートアクセス モードを有効にする必要があります。

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（onfiguration）]** の順に選択します。

ステップ 2 **[Unified Communicationsモード（Unified Communications mode）]** を **[モバイルおよびリモートアクセス（Mobile and Remote Access）]** に設定します。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 Expressway-E でこの手順を繰り返します。

MRA 経由の IPv6 の有効化

Expressway-E 外部 LAN を設定して、デュアルアドレッシングをサポートします。この設定により、Expressway が MRA 経由の IPv6 をサポートできるようになります。

Expressway X14.2 リリースは、IPv6 経由の MRA クライアントを正式にサポートするようになりました。このサポートは、以前は利用できませんでした。ただし、このサポートを提供するには、Expressway、CUCM、およびその他のネットワークコンポーネントでいくつかの設定変更が必要です。

- 「両方」としてのデュアルネットワーク オプションで Expressway-Edge を有効にします。
- グローバルユニキャスト IPv6 アドレスを使用して、MRA クライアントとの外部通信に使用されるインターフェイスを構成します。
- DNS には、Exp-E の IPv6 アドレスを解決するための有効な AAAA レコードが必要です。MRA クライアントは、「collab-edge_tls」dns srv クエリ中にこれを返します。
- デュアルネットワーク用に CUCM/IMP サーバーを設定します。これらのサーバーに IPv6 アドレスを設定する必要はありません。

ドメインの追加

Expressway-C で、MRA 展開が使用するドメインを追加します。システムの複雑さに応じて、これは単一の企業全体のドメインになる場合もあれば、次のような複数のドメインになる場合もあります。

- 企業ドメイン
- 内部 UC ドメイン（企業ドメインと異なる場合）
- エッジドメイン（他のドメインと異なる場合）
- プレゼンスドメイン（他のドメインと異なる場合）

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[ドメイン（Domains）]**の順に選択します。

ステップ 2 **ドメイン名**を入力します。

ステップ 3 次の各サービスの場合、サービスをこのドメインに適用するかどうかに応じて、対応するドロップダウンを **[オン]** か **[オフ]** にします。

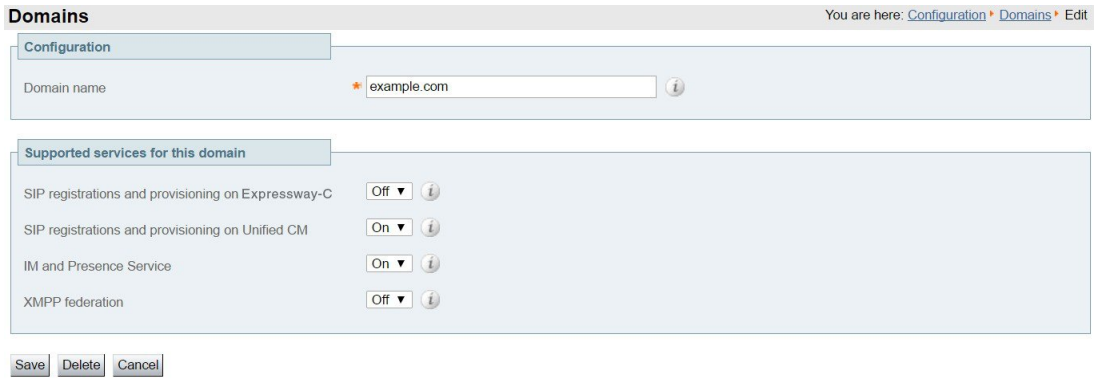
- **Expressway での SIP 登録およびプロビジョニング**—Expressway は、SIP レジストラとして機能し、任意の SIP ドメインの登録リクエストを承認します。
- **Unified CM での SIP 登録およびプロビジョニング**—Unified CM が終了登録と呼制御を処理します。Expressway は、UC サービスのゲートウェイとして機能します。
- **IM and Presence Service**—クライアントが IIM and Presence Service からサービスを取得します。
- **XMPP フェデレーション**—このドメインとパートナードメイン間で、XMPP フェデレーションを有効化します。

ステップ 4 複数の**展開**を構成した場合、このドメインを適用する展開を割り当てます。このフィールドは、複数ドメインを構成した時のみ表示されることに注意してください。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 追加を追加する場合はこの手順を繰り返します。

図 *1:* ドメイン



Unified CM クラスタの追加

Expressway-C から各 Cisco Unified Communications Manager クラスタに接続を確立するには、この手順を使用します。各 Expressway-C クラスタは、各 Unified CM クラスタノードに到達できる必要があります。

（注）

- Expressway-C は、TLS 検証モードがオンの場合、ICMP を使用して CUCM に接続します。CUCM と Expressway-C の間のネットワークで ICMP が許可されていることを確認します。
- 登録エンドポイントにルーティング情報を戻す際、Unified CM が負荷分散を管理します。
- 負荷は、リソースの使用状況に基づいてノード全体に分散されます。エンドポイントは、Cisco Unified Communications Manager に到達するために最も負荷の少ないノードを受け取ります。コールのロードバランシングはなく、最初の登録のみが負荷分散されます。登録が負荷分散されるため、単一ノードでのコールの過負荷の可能性が減少します。
- 現在、MRA でサポートされている Cisco Unified CM/IM and Presence/Cisco Unity Connection サーバークラスタの最大制限数は公開されていません。単一の Expressway ノードは、400 を超える UCM ノードを処理できません。CUCM は、単一の中規模 OVA Expressway で 20 のクラスタをサポートします。これには、さまざまな展開サイズは含まれません。

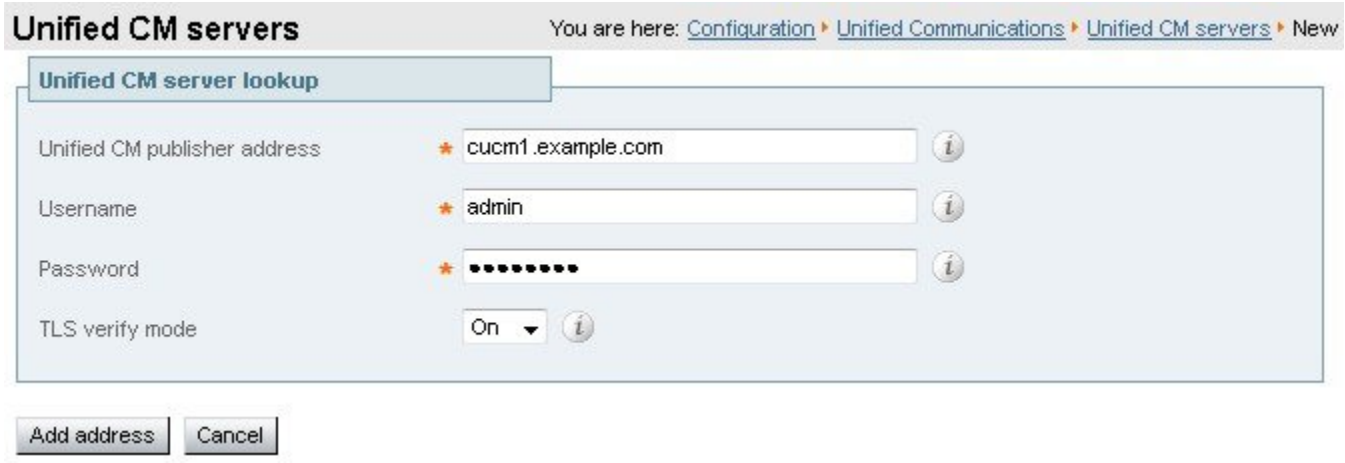
ステップ 1 Expressway-C プライマリピアで、**[構成（Configuration）]** > **[Unified Communications]** > **[Unified CMサーバー（Unified CM servers）]** の順に選択します。

ステップ 2 **[新規（New）]** をクリックし、パブリッシャノードに関する次の詳細を追加します。

- **Unified CM パブリッシャアドレス**—パブリッシャノードのサーバーアドレス
- **ユーザー名**と**パスワード** —サーバーにアクセスできるアカウントのユーザー ID とパスワード。

  （注） これらのログイン情報は、Expressway データベースに恒久的に保管されます。対応する Unified CM ユーザーには、Standard AXL API Access ロールが必要です。

- **TLS 検証モード**
- **AEM GCM メディア暗号が**—AEM GCM サポートを有効化するには、これをオンにします。
- **展開**—複数の展開を構成した場合は、該当する展開を選択します。このフィールドは、展開を構成していない限り表示されません。



ステップ 3 **[アドレスを追加（Add Address）]** をクリックして、接続をテストします。

ステップ 4 複数の Unified CM クラスタがある場合は、手順 2 と 3 を繰り返して、追加の Unified CM クラスタのパブリッシャノードをこの Expressway-C クラスタに追加します。

ステップ 5 すべての Unified CM パブリッシャノードを追加したら、**[サーバーを更新（Refresh Servers）]** をクリックします。
Expressway-C は、各クラスタのサブスクライバノードを検出して追加します。

ステップ 6 Expressway-C クラスタが複数場合は、すべての Expressway-C クラスタがすべての Unified CM クラスタおよびノードに接続できるようになるまで、他の Expressway-C クラスタでこの手順を繰り返します。

自動生成されたゾーンと検索ルール

Expressway-C は、Expressway-C と検出された各 Unified CM ノード間で構成できないネイバーゾーンを自動生成します。TCP ゾーンは常に作成されます。TLS ゾーンは、Unified CM ノードがクラスタセキュリティモード（**[システム（System）]** > **[企業パラメータ（Enterprise Parameters）]** > **[セキュリティパラメータ（Security Parameters）]**）が 1（混合）で構成されている場合に作成されます（これにより、セキュアなプロファイルでプロビジョニングされたデバイスがサポートされます）。TLS ゾーンは、Unified CM が TLS 検証モードを有効になっている場合、**[TLS検証モード（TLS verify mode）]** が **[オン（On）]** の状態で構成されます。これは、Expressway-C が後続の SIP 通信用の CallManager 証明書を確認することを意味します。各ゾーンは「CEtcp-<node name>」または「CEtls-<node name>」の形式で作成されます。

X12.5 バージョンから、Unified CM 上で SIP OAuth モードが有効になっている場合、Expressway は、自身と検出された Unified CM ノード間に「CEOAuth <Unified CM name>」という名前のネイバーゾーンを自動的に生成します。詳細については、SIP OAuth モードの設定 （21 ページ）を参照してください。

また、同じ命名規則に従って、構成不可能な検索ルールが各ゾーンに自動作成されます。ルールは 45 の優先順位で作成されます。検索ルールの対象となる Unified CM ノード名が長い場合、検索ルールは正規表現を使ってアドレスのパターンマッチを行います。

IM and Presence Service クラスタの追加

この手順を使用して、Expressway-C から各 IM and Presence Service クラスタへの接続を作成します。各 Expressway-C クラスタは、各 IM and Presence Service クラスタ ノードに到達できる必要があります。

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[IM and Presenceサービスノード（IM and Presence Service nodes）]** の順に選択します。

ステップ 2 **[新規（New）]** をクリックし、データベース パブリッシャ ノードに関する次の詳細を追加します。

- **IM and Presence データベースパブリッシャ名**ーデータベース パブリッシャ ノードのサーバーアドレス
- **ユーザー名**と**パスワード** — サーバーにアクセスできるアカウントのユーザー ID とパスワード。

  （注） これらのログイン情報は、Expresswayデータベースに恒久的に保管されます。対応する IM and Presence Service ユーザーには、Standard AXL API Access ロールを付与する必要があります。

- **TLS 検証モード**
- **展開**—複数の展開を構成した場合は、該当する展開を選択します。

  （注） このフィールドは、展開を構成していない限り表示されません。

ステップ 3 **[アドレスを追加（Add Address）]** をクリックして、接続をテストします。

ステップ 4 複数の IM and Presence クラスタがある場合は、手順 2 と 3 を繰り返して、これらの追加クラスタのデータベース パブリッシャ ノードを Expressway-C クラスタに追加します。

ステップ 5 すべての IM and Presence データベース パブリッシャ ノードを追加したら、**[サーバーを更新（Refresh Servers）]** をクリックします。
Expressway-C は、各 IM and Presence クラスタのサブスクライバノードを検出して追加します。

ステップ 6 複数の Expressway-C クラスタがある場合は、各 Expressway-C クラスタが各 IM and Presence クラスタノードに接続されるまで、他の Expressway-C クラスタでこの手順を繰り返します。

Cisco Unity Connection クラスタの追加

この手順を使用して、Expressway-Cから各Cisco Unity Connectionクラスタへの接続を作成します。各 Expressway-C クラスタは、各 Cisco Unity Connection クラスタノードに到達できる必要があります。

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[Unity Connection サーバー（Unity Connection servers）]**の順に選択します。

ステップ 2 **[新規（New）]** をクリックし、パブリッシャノードの次の詳細を追加します。

- **Unity Connection パブリッシャ名** — パブリッシャノードのサーバーアドレス
- **ユーザー名**と**パスワード** — サーバーにアクセスできるアカウントのユーザー ID とパスワード。

  （注） これらのログイン情報は、Expressway データベースに恒久的に保管されます。対応する Cisco Unity Connection ユーザーには、システム管理者ロールが必要です。

- **TLS 検証モード**
- **展開**—複数の展開を構成した場合は、該当する展開を選択します。

  （注） このフィールドは、展開を構成していない限り表示されません。

ステップ 3 **[アドレスを追加（Add Address）]** をクリックして、接続をテストします。

ステップ 4 複数の Unity Connection クラスタがある場合は、手順 2 と 3 を繰り返して、それらの追加クラスタのパブリッシャノードをこの Expressway-C クラスタに追加します。

ステップ 5 この Expressway-C にすべての Unity Connection クラスタを追加したら、**[サーバーを更新（Refresh Servers）]** をクリックします。
Expressway-C は、各クラスタのサブスクライバノードを検出して追加します。

ステップ 6 複数の Expressway-C クラスタがある場合は、各 Expressway-C クラスタが各 Unity Connection クラスタノードに接続されるまで、他の Expressway-C クラスタでこの手順を繰り返します。

MRA アクセス制御の構成

クライアントがモバイルおよびリモートアクセス（MRA）リクエストを認証する方法を定義します。

⚠

注意 X8.9 以前からアップグレードする場合は、アップグレード後に適用された設定はここで一覧されているものとは異なります。代わりに、「Expressway リリースノート」のアップグレード指示を参照してください。

ステップ 1 Expressway-C で、**[設定（Configuration）]** > **[Unified Communications]** > **[設定(Configuration)]** > **[MRAアクセスコントロール（MRA Access Control）]** に移動します。

ステップ 2 認証設定の構成

- **[認証パス（Authentication Path）]** フィールドで、SAML、SSO、LDAP または ローカルデータベースを使用して、認証ユーザーログイン情報を認証するかどうかを選択します。
- **[OAuthトークンで認証（Authorize by OAuth token）]** を選択すると Expressway で OAuth 認証が有効化されます。このオプションは、SAML SSO でのみサポートされています。

ステップ 3 追加フィールドを構成します。フィールド設定についての詳細は、「Expressway（Expressway-C）アクセス制御の設定 （11 ページ）」を参照してください。

Expressway（Expressway-C）アクセス制御の設定

次の表に MRA アクセス制御（**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** > **[MRA アクセス制御（MRA Access Control）]**）で表示される説明を示します。この構成ページを使用して、モバイルおよびリモートアクセスの OAuth 認証設定と SAML SSO 設定を構成できます。

表 *1 : MRA* アクセス制御の設定

フィールド	説明
認証パス（Authentication path）	MRA が有効になるまで非表示のフィールド。MRA 認証の制御方法を定義します。 • **SAML SSO 認証**—クライアントは、外部 IdP によって認証されます。 • **UCM/LDAP Basic 認証**—Unified CM が、LDAP ログイン情報に対してクライアントをローカルで認証します。 • **SAML SSO および UCM/LDAP**—両方のメソッドを許可します。 • **[なし（None）]**—認証が適用されていません。MRA が最初に有効になるまでは、これがデフォルトです。単に MRA をオフにするのではなく「[なし（None）]」 オプションが用意されているのは、展開によっては、実際には MRA ではない機能を許可するために MRA をオンにする必要があるためです。（Meeting Server の Web プロキシ、XMPP フェデレーションなど）。[なし（None）]「」は、そのような場合にのみ使用してください。**それ以外の場合はお勧めしません。** デフォルト設定：MRA がオンになる前は **[なし（None）]**。MRA をオンにすると、デフォルト値は、**UCM/LDAP** になります。

フィールド	説明
OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）	このオプションでは、承認のための自己記述トークンが必要です。サポート用のインフラストラクチャを持つすべての展開で推奨される承認オプションです。 OAuth は、 Cisco Jabber および Cisco Webex クライアントおよび MRA モードでデバイスアクティベーションコードを使用して導入準備をする Cisco IP Phones によってサポートされています。 **重要**：X8.10.1 から、Expressway は自己記述トークン（トークン更新、高速承認、アクセスポリシーサポートを含む）の利点を完全にサポートしています。ただし、実際にはすべての利点が広範なソリューション全体で利用できるわけではありません。使用する他の製品（Unified CM、IM and Presence Service、Cisco Unity Connection）およびそのバージョンによって、すべての製品が自己記述トークンのすべての利点を完全にサポートしているわけではありません。 Expressway でこのオプションを使用する場合は、**Unified CM および使用されている場合は Cisco Unity Connection で OAuth を更新して有効にする必要もあります**。このプロセスの概要は次のとおりです。 デフォルト設定：オン
OAuth トークンによる承認 （以前は SSO モード）	**[認証パス（Authentication path）]** がSAML SSO または SAML SSO および UCM/LDAP の場合、利用可能。 このオプションには、IdP を使用した認証が必要です。現在、 Cisco Jabber および Cisco Webex クライアントのみが、この認証方式を使用しており、これは別の MRA エンドポイントではサポートされていません。 デフォルト設定：オフ
ユーザ クレデンシャルによる承認（Authorize by user credential）	**[認証パス（Authentication path）]** が UCM/LDAP または SAML SSO および UCM/LDAP の場合、利用可能。 ユーザクレデンシャルによる認証を実行しようとするクライアントは、MRA によって許可されます。これには、Jabber、サポートされている IP 電話機および TelePresence デバイスが含まれます。 デフォルト設定：オフ
ID プロバイダー：IdP の作成または変更（Identity providers: Create or modify IdPs）	**[認証パス（Authentication path）]** が SAML SSO または SAML SSO および UCM/LDAP の場合、利用可能。 詳細については、アイデンティティ プロバイダーの選択 （19 ページ）を参照してください。

フィールド	説明
SAML メタデータ（SAML Metadata）	**[認証パス（Authentication path）]** が SAML SSO または SAML SSO および UCM/LDAP の場合、利用可能。 SAML 契約のメタデータファイルを生成する方法を決定します。設定可能なモードは、次のとおりです。 • **クラスタ**：単一のクラスタ全体の SAML メタデータファイルを生成します。SAML 契約のために、このファイルのみを IdP にインポートする必要があります。 • **ピア**：クラスタ内の各ピアに対してメタデータファイルを生成します。SAML 契約のために、各メタデータファイルを IdP にインポートする必要があります。
ID プロバイダー：SAML データのエクスポート（Identity providers: Export SAML data）	**[認証パス（Authentication path）]** がSAML SSO または SAML SSO および UCM/LDAP の場合、利用可能。 SAML データの操作の詳細については、「エッジ経由の SAML SSO 認証（15 ページ）」を参照してください。
Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）	iOS デバイスの場合、IdP または Unified CM 認証ページは、デフォルトで組み込み Web ブラウザ（Safari ブラウザではない）で表示されます。このデフォルトのブラウザは iOS の信頼ストアにアクセスできないので、デバイスに導入された証明書を使用することはできません。 この設定は、ネイティブ Safari ブラウザを使用するよう iOS デバイスの Jabber をオプションで許可します。Safari ブラウザでは、デバイスの信頼ストアにアクセスできるため、OAuth 導入時にパスワードレス認証または二要素認証を有効化できるようになりました。 このオプションには潜在的なセキュリティの問題が存在します。認証が完了した後で、Safari から Jabber にブラウザ制御を返す機能は、カスタム プロトコル ハンドラを呼び出すカスタム URL 方式を使用します。Jabber 以外の別のアプリケーションがこの方式を妨害し、iOS から制御を取得できます。この場合、アプリケーションは URL の OAuth トークンへアクセスできます。 すべてのモバイルデバイスが管理されているなどの理由で、iOS デバイスに Jabber のカスタム URL 形式を登録する他のアプリケーションがないと確信する場合、オプションを有効にしても安全です。別のアプリケーションがカスタム Jabber URL を妨害する可能性が心配な場合、組み込み Safari ブラウザを有効に**しない**でください。 デフォルト設定：いいえ

フィールド	説明
内部認証の可用性の確認（Check for internal authentication availability）	[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）] または [OAuth トークンによる承認（Authorize by OAuth token）] が有効になっている場合に利用可能。 最適なセキュリティとネットワーク トラフィックの削減のため、デフォルトは [いいえ（No）] です。 Expressway-C がホーム ノードをチェックするかどうかを選択することにより、Expressway-E がリモートクライアント認証要求にどのように反応するかを制御します。 リクエストは、クライアントが OAuth トークンによってユーザを認証しようとする可能性があるかどうかを尋ね、そのリクエストには Expressway-C がユーザのホーム クラスタを見つけるためのユーザ ID が含まれています。 • はい：*get_edge_sso* リクエストは、OAuth トークンがサポートされているかどうかをユーザーのホーム Unified CM に確認します。ホーム Unified CM は、Jabber クライアントの *get_edge_sso* リクエストが送信するアイデンティティで判断します。 • いいえ（No）：Expressway が内部を参照しないように構成されている場合に、Edge の認証設定に応じて、すべてのクライアントに同じ応答が送信されます。 選択するオプションは、実装およびセキュリティ ポリシーによって異なります。すべての Unified CM ノードが OAuth トークンをサポートする場合、*[いいえ（No）]* を選択すると応答時間とネットワーク全体のトラフィックを削減できます。または、ロールアウト中にクライアントがエッジ構成を取得するモードを使用するようにする場合や、すべてのノードで OAuth を保証できない場合は、*[*はい（*Yes*）*]* を選択します。 **注意：これを [はい（Yes）] に設定すると、認証されていないリモート クライアントからの不正なインバウンド要求が許可される可能性があります。**この設定に [いいえ（No）] を指定すると、Expressway は不正なリクエストを防止します。 デフォルト設定：いいえ
アクティベーションコードの導入準備を許可（Allow activation code onboarding）	**[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** または **[OAuth トークンによる承認（Authorize by OAuth token）]** が有効になっている場合のみに利用可能。この設定により、Expressway のアクティベーションコードによる導入準備が有効になります。デフォルト値は **[いいえ（No）]** です。このオプションを有効にするには値を **[はい（Yes）]** に設定します。 デフォルト設定：いいえ

フィールド	説明
SIP トークンの余分なパケット存続時間（SIP token extra time to live）	[OAuth トークンによる承認（Authorize by OAuth token）] が [オン（On）] の場合に利用可能。 必要に応じて、簡単な OAuth トークンの存続可能時間（秒）を延長します。クレデンシャルの有効期限が切れた後、コールを受け入れるための短い時間枠をユーザに提供します。ただし、潜在的なセキュリティ リスクが増加します。 デフォルト設定：0 秒
Webex クライアント埋め込みブラウザサポート（WebEx Client Embedded Browser Support）	SSO リダイレクト URI を送信する Jabber および Webex クライアントに適用されます。 デフォルト値：いいえこのオプションを有効にするには値を [はい（Yes）] に設定します。 この機能により、Jabber と Webex クライアント組み込みブラウザサポートのセキュリティが強化されます。これにより、クライアントは、Unified Communications Manager（および MRA）OAuth フロー向けの埋め込みブラウザを使用できるようになり、ユーザーエクスペリエンスが改善されます。

（注） Expressway では、Unified CM サーバーがサポートする認証方法を確認できます。使用中のバージョン番号が表示されます。

Expressway で、**[構成（Configuration）] > [Unified Communications] > [Unified CMサーバー（Unified CM servers）]**の順に選択します。

エッジ経由の SAML SSO 認証

SAML ベースの SSO は、Unified Communications サービスリクエストを認証するためのオプションです。要求は、企業ネットワーク内、または（ここで説明されているように）外部から MRA 経由で Unified Communications サービスを要求するクライアントから発信されます。

エッジ経由の SAML SSO 認証には、**外部**アイデンティティ プロバイダー（IdP）が必要です。その認証は、エッジでの Expressway ペアのセキュアなトラバーサル機能と、内部のサービス プロバイダーと外部で解決可能なアイデンティティ プロバイダー（IdP）との間の信頼関係に依存します。

エンドポイントは VPN 経由で接続する必要はありません。これらは、複数の Unified Communications サービスにアクセスするために、1 つのアイデンティティと 1 つの認証メカニズムを使用します。認証は IdP によって所有され、 Expressway の認証も内部 Unified CM サービスもありません。

Expressway は、SAML SSO を使用した 2 種類の OAuth トークン認証をサポートします。

- シンプル（標準）なトークン。これらは常に SAML SSO 認証を必要とします。

- 更新を伴う自己記述トークン。これらは、Unified CM ベースの認証でも機能します。

（注）
- Jabber エンドポイントが更新なしで SSO を使用し、最初に Expressway/MRA を介してリモートで Unified CM を認証してからローカルネットワークに戻る場合、エンドポイント（エッジからオンプレミス）に再認証は必要ありません。
- Jabber エンドポイントが最初にローカルネットワークで Unified CM に直接認証し、次に Expressway/MRA を使用して Unified CM にリモートでアクセスする場合、エンドポイント（オンプレミスからエッジ）に再認証が必要です。

簡易 OAuth トークン認証について

前提条件

- Cisco Jabber 10.6 以降。Jabberクライアントは、モバイルおよびリモートアクセス（MRA）を介する OAuth トークン認証をサポートする唯一のエンドポイントです。
- Cisco Unified Communications Manager 10.5 (2) 以降
- Cisco Unity Connection 10.5 (2) 以降
- Cisco Unified Communications Manager IM and Presence Service 10.5(2) 以降

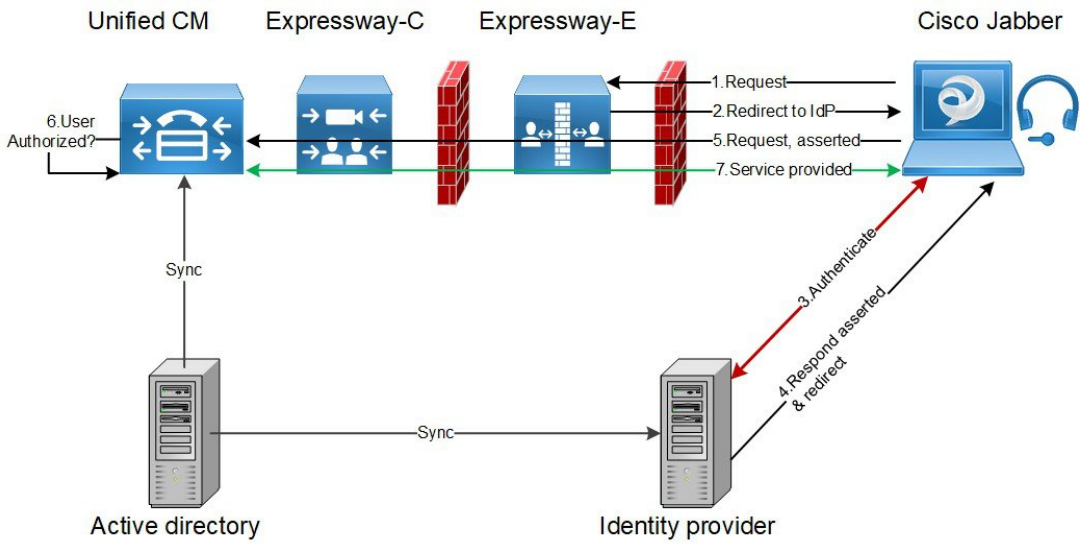
仕組み

Cisco Jabber は、ユニファイド コミュニケーション サービスを要求する前に、組織のネットワーク内にあるかどうかを判定します。Jabber がネットワークの外側にいる場合は、ネットワークのエッジにある Expressway-E からサービスを要求します。認証がエッジで有効な場合、Expressway-E はユーザーを認証するために署名した要求を使用して Jabber を IdP にリダイレクトします。

IdP は、クライアント自体を識別するためにクライアントにチャレンジを行います。このアイデンティティが認証されると、IdP は、Jabber のサービスリクエストを、アイデンティティが本物であるという署名済みアサテーションを付けて、Expressway-E にリダイレクトします。

Unified Communications サービスが、IdP と Expressway-E を信頼すると、サービスを Jabber クライアントに提供します。

図 *2*:オンプレミス *UC* サービスに対するシンプルな *OAuth* トークンベースの承認



更新を伴う自己記述 OAuth トークン承認について

Expressway は、X8.10.1 からの MRA 承認オプションとしての自己記述トークンを使用してサポートします。（**[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** を **[はい（Yes）]** に設定します。）自己記述トークンには、次のように大きな利点があります。

- トークン更新機能により、ユーザーは繰り返し再認証する必要がありません。
- 迅速な承認。
- アクセスポリシーのサポート。Expressway は、Unified CM のユーザーに適用された MRA アクセスポリシー設定を強制できます。
- ローミングのサポート。トークンはオンプレミスでもリモートでも有効なので、ローミングユーザーはオンプレミスとオフプレミスの間を移動する場合に再認証する必要がありません。
- Expressway-C はホスト名を提供しますが、Unified CM は（Expressway-C 証明書 CN/SAN で発行されたように）Expressway-C FQDN を解決できる必要があります。これは、分割ドメインネームシステム（DNS）環境に特に関連します。Unified CM **管理** > **デバイス** > **Expressway-C**で、それらが FQDN として定義されていることを確認します。また、ローカル DNS が Expressway C の FQDN を解決できるかどうかを確認します。

  Unified CM サーバーが Expressway C からいつでも更新されると、ホスト名が再挿入されます。FQDN とホスト名の両方があり、問題が発生します。そのため、ホスト名を削除します。

Expressway は、特に Cisco Jabber ユーザーを円滑に進めるため、自己記述トークンを使用します。モバイルまたははリモートの Jabber ユーザーは、ローカルネットワーク（オフプレミス）

から離れていても認証できます。ユーザーが元々オンプレミスで認証していた場合、後でオフプレミスに移動した場合に再認証する必要はありません。同様に、ユーザーがオフプレミスで認証した後にオンプレミスに移動した場合、ユーザは再認証する必要はありません。どちらの場合も、構成されたアクセストークンまたは更新トークン制限の対象となり、再認証が適用される可能性があります。

Jabber iOS デバイスを使用するユーザーの場合、自己記述トークンでサポートされている高速度が、Apple Push Notifications（APN）の Expressway サポートを最適化します。

自己記述トークン承認をサポートするために必要なインフラストラクチャがあることを前提として、すべての展開に対して自己記述トークン承認を推奨します。適切な Expressway 構成に従い、Jabber クライアントが、自己記述トークンを提示した場合、Expressway は単純にトークンを確認します。パスワードまたは証明書ベースの認証は必要ありません。構成された認証パスが外部 IdP によるものか、または Unified CM によるものかにかかわらず、トークンは Unified CM によって発行されます。コールフロー内のすべてのデバイスが自己記述トークン承認用に構成されている場合、自己記述トークン承認が自動的に使用されます。

Expressway-C は、トークン認証を実行します。これにより、認証と認証設定が Expressway-E で公開されるのを回避します。

前提条件

- Expressway は、すでに Cisco Jabber に対してモバイルおよびリモートアクセスを提供しています。
- コール フロー内の他のすべてのデバイスも同様に有効化されます。
- 次の最小製品バージョン（またはそれ以降）がインストールされている。
  - Expressway X8.10.1
  - Cisco Jabber iOS 11.9

    最大 Jabber デバイスを保持していて、その一部が古いソフトウェアバージョンの場合、古いソフトウェアバージョンは、単純な OAuth トークン認証を使用します（SSO と IdP が設定されていることが前提）。
  - Cisco Unified Communications Manager 11.5(SU3)
  - Cisco Unified Communications Manager IM and Presence Service 11.5(SU3)
  - Cisco Unity Connection 11.5(SU3)
- 自己記述認証が Cisco Expressway-C（**[OAuthトークン（更新あり）（OAuth token with refresh）]** 設定で認証）および Unified CM および/または IM and Presence Service（**OAuth with Refresh Login Flow** 企業パラメータ）でオンであることを確認します。
- Expressway で定義した Unified CM ノードを更新する必要があります。これにより、Expressway がトークンを復号化する Unified CM からキーをフェッチできます。

OAuth トークンの前提条件

このトピックでは、OAuth トークンに関して展開が満たす必要のある前提条件について説明します。

Expressway Pair 上

- Expressway-E と an Expressway-C はネットワークエッジで連携するように構成されています。
- Unified Communications トラバーサルゾーンは、Expressway-C と Expressway-E の間で構成されています。
- OAuth 経由でアクセスする SIP ドメインは、Expressway-C で構成されています。
- Expressway-C では MRA が有効化されており、必要な Unified CM リソースが検出されています。
- 必要な Unified CM リソースは、Expressway-C の HTTP 許可リストにあります。
- 複数の展開を使用する場合、OAuth がアクセスする Unified CM リソースは、Jabber クライアントからコールされるドメインと同じ展開にあります。

Cisco Jabber クライアント上

- クライアントは、正しいドメイン名/SIP URI/チャットエイリアスを使用して内部サービスを要求するように構成されている。
- デフォルトブラウザは Expressway-E および IdP を解決できます。

Unified CM での手順

非 OAuth MRA クライアントやエンドポイントに関連付けられているユーザーは、Unified CM にログイン情報を保存しています。または、Unified CM は、LDAP 認証用に構成されています。

アイデンティティ プロバイダー上

IdP 証明書のドメインは、クライアントが IdP を解決できるように、ドメインネームシステム（DNS）で公開する必要があります。

アイデンティティ プロバイダーの選択

シスコ コラボレーション ソリューションは、SAML 2.0（セキュリティ アサーション マークアップ言語）を使用して、ユニファイド コミュニケーション サービスを利用するクライアント用の SSO（シングル サインオン）を有効にします。

使用する環境に SAML ベース SSO を選択した場合は、次の点に注意してください。

- SAML 2.0 は、SAML 1.1 との互換性がないため、SAML 2.0 標準を使用する IdP を選択する必要があります。

- SAMLベースのアイデンティティ管理は、コンピューティングとネットワーキング業界のベンダーによって異なる方法で実装されています。したがって、SAML標準に準拠するための幅広く受け入れられている規制はありません。
- 選択した IdP の設定や管理ポリシーは、Cisco TAC（テクニカル アシスタンス センター）のサポート対象外です。IdP ベンダーとの関係とサポート契約を利用して、IdP を正しく設定するアシストを受けてください。Cisco は IdP に関するエラー、制限、または特定の設定に関する責任を負いません。

シスコ コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、シスコ コラボレーション ソリューションでテストされているのは次の IdP だけです。

- OpenAM 10.0.1
- Active Directory Federation Services 2.0（AD FS 2.0）
- PingFederate® 6.10.0.4
- Okta、Azure、F5 BIG IP

UC アプリケーションで OAuth を構成する

Expressway で MRA を使用して OAuth 認証を使用するには、Cisco Unified Communications Manager や Cisco Unity Connection（導入されている場合）などの内部 UC アプリケーションでも OAuth 認証を有効にする必要があります。

ステップ 1 Expressway-C で、MRA アクセス制御設定で OAuth トークンの更新が有効になっていることを確認します。

a) Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** > **[MRAアクセス制御（MRA Access Control）]** の順に選択します。
b) **[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** チェックボックスをオンにします。
c) [保存（Save）] をクリックします。

ステップ 2 Cisco Unified Communications Manager パブリッシャノードで、**OAuth Refresh Login Flow** 企業パラメータを有効にします。

a) Cisco Unified CM Administration から、**[システム（System）]** > **[企業パラメータ（Enterprise Parameters）]** を選択します。
b) **OAuth with Refresh Login Flow** パラメータを **[有効（Enabled）]** に設定します。
c) [保存（Save）] をクリックします。

（注） Expressway が Cisco Unified Communications Manager とは異なるドメインで設定されている場合、Cisco Unified Communications Manager 管理者は、Exp-C の関連するシステムドメインを追加することにより、Exp-C ホスト名エントリを手動で FQDN に更新する必要があります。

ステップ 3 Cisco Unity Connection で、OAuth 更新ログインを有効にし、Authz サーバーを構成します 。

a) Cisco Unity Connection Administration から、**[システム設定（System Settings）]** > **[エンタープライズパラメータ]** を選択します。
b) **[SSO および OAuth 設定]** の下で設定を構成します。
c) **[更新ログイン フローを使用した OAuth（OAuth with Refresh Login Flow）]**エンタープライズ パラメータ を **[有効（Enabled）]** に設定します。
d) [保存（Save）] をクリックします。
e) **[システム設定（System Setting）]** > **[Authzサーバー（Authz Server）]**の順に選択します。
f) 既存の構成を編集するか、新しい Authz サーバーを追加します。
g) Authz サーバー設定に **Cisco Unified Communications Manager パブリッシャ**を追加します。
h) [保存（Save）] をクリックします。

次のタスク

システムが必要な要件を満たしている場合は、Cisco Unified Communications Manager で SIP OAuth モードを有効にします。

SIP OAuth モードの設定

この手順を使用して、Cisco Unified Communications Manager で SIP OAuth モードを有効にします。SIP OAuth モードは、安全な SIP 回線シグナリングが必要であり、システムがそれをサポートしている場合にお勧めします。

（注） X14.0 リリースから、SIP OAuth モードは 7800 および 8800 シリーズの Cisco IP Phone でサポートされます。SIP OAuth モードの詳細情報に関しては、『*Cisco Unified Communications Manager* の機能構成ガイド』の「SIP OAuth モードの構成」章を参照してください。

始める前に

Cisco Unified Communications Manager で、OAuth 更新ログインを有効にする必要があります。これは、**OAuth with Refresh Login Flow** 企業パラメータを **[有効（Enabled）]** にすることで設定できます。

ステップ 1 SIP OAuth を使用するサーバーごとに、SIP OAuth ポートを設定します。
a) Cisco Unified CM Administration で、**[システム（System）]** > **[Cisco Unified CM]** の順に選択します。
b) **[TCPポート設定（TCP Port Settings）]** を設定します。
c) [保存（Save）] をクリックします。

ステップ 2 Expressway-C への OAuth 接続の構成方法
a) Cisco Unified CM Administration で、**[デバイス（Device）]** > **[Expressway-C]**の順に選択します。
b) **[新規追加（Add New）]** をクリックします。
c) Expressway-C アドレスの追加

d) [保存（Save）] をクリックします。

ステップ 3 SIP OAuth モードを有効にする方法

a) ノードで、コマンド ライン インターフェイスにログインします。

b) `utils sipOAuth-mode enable` の CLI コマンドを実行します。

ステップ 4 **Cisco CallManager** サービスを再起動する方法

a) Cisco Unified Serviceability で、**[ツール（Tools）] > [コントロールセンター - 機能サービス（Control Center - Feature Services）]**の順に選択します。

b) **[サーバ（Server）]** ドロップダウン リストからサーバを選択します。

c) **Cisco CallManager** サービスを確認し、[再起動（Restart）] をクリックします。

d) エンドポイントが SIP OAuth モードで登録する各ノードを再起動します。

ステップ 5 電話機セキュリティプロファイルで OAuth 認証を有効化します。

a) Cisco Unified CM Administration で**[システム（System）] > [セキュリティプロファイル（Security Profile）] > [電話機セキュリティプロファイル（Phone Security Profile）]**の順に選択します。

b) **[検索（Find）]** をクリックして、MRA エンドポイントに関連付けられているプロファイルを選択します。

c) [OAuth 認証の有効化（Enable OAuth Authentication）] チェックボックスをオンにします。

d) ICE Media Path Optimization を使用している場合は、**[デバイスセキュリティモード（Device Security Mode）]** を **[暗号化（Encrypted）]** に設定し、**[転送タイプ（Transport Type）]** を **[TLS]** に設定します。

e) [保存（Save）] をクリックします。

SAML SSO の設定

モバイルおよびリモートアクセス用に Cisco Expressway で SAML SSO を設定する場合は、次のタスクを実行します。

始める前に

- 内部 UC アプリケーション用に SAML SSO を構成します。詳細については、『シスコ ユニファイド コミュニケーション ソリューション用*SAML SSO*導入ガイド』を参照してください。
- Expressway-C の MRA アクセス制御設定では、**[認証パス（Authentication path）]** フィールドを **[SAML SSO認証（SAML SSO authentication）]** または **[SAML SSOおよびUCM/LDAP（SAML SSO and UCM/LDAP）]** に設定する必要があります。

注意 次の変更では、SAML メタデータを更新する必要があります。

- Expressway の変更：Expressway-C 証明書、FQDN、クラスタの追加 (メタデータを送信して再度インポート)
- IDP の変更：FQDN、証明書、またはクライアントとの信頼関係に影響を与えるもの（最新のメタデータを再インポート）

手順

	コマンドまたはアクション	目的
ステップ 1	Expressway-C から SAML メタデータをエクスポート（23 ページ）	Expressway-C から メタデータファイルをエクスポートします。
ステップ 2	アイデンティティ プロバイダの設定	Expressway メタデータをアイデンティティ プロバイダー（IdP）にインポートし、IdP を設定してから、IdP からメタデータファイルをエクスポートします。
ステップ 3	IdP から SAML メタデータをインポート （25 ページ）	Idp メタデータを Expressway-C にインポートし、構成を完了します。
ステップ 4	IdP とドメインの関連付け （25 ページ）	Expressway-C で、ドメインをアイデンティティ プロバイダーに関連付けます。
ステップ 5	SAML SSO に ADFS を構成 （26 ページ）	ADFS のみ。Active Directory フェデレーションサービスを使用している場合は、IdP でこれらの追加タスクを完了して構成を完了します。

Expressway-C から SAML メタデータをエクスポート

X12.5 から Cisco Expressway は、IdP との SAML 契約に対して単一のクラスタ全体のメタデータファイルを使用することをサポートしています。以前は、Expressway-C クラスタのピアごとにメタデータファイルを生成する必要がありました (たとえば、6 つのメタデータファイルなど)。クラスタ全体のオプションの場合、Expressway-C プライマリ ピアでこの手順を実行します。

（注）

- SAML SSO 展開で次のいずれかの Expressway 設定を変更する場合は、メタデータをプライマリピアから再エクスポートし、メタデータを IdP に再インポートする必要があります。
  - プライマリピア
  - サーバー証明書
  - SSO 対応ドメイン
  - Expressway-E ピアの IP アドレスまたはホスト名
- Expressway-C の SAML メタデータをエクスポートする前に、Expressway-C で、Expressway-E との有効な接続を確立する必要があります。
- Expressway を新しいアプライアンスまたは仮想マシンに再展開し、元の Expressway からバックアップを復元した場合、「SAML メタデータが変更されました（SAML metadata is modified）」というアラームが発生します。**[ダウンロード（Download）]** を選択してアラームをクリアします。他の変更を行っていない場合は、IDP を更新する必要はありません。

ステップ 1 **[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** の順に選択します。

ステップ 2 **[MRAアクセス制御（MRA Access Control）]** セクションの SAML メタデータリストでモードを選択します。

- **クラスタ**：単一のクラスタ全体の SAML メタデータファイルを生成します。このファイルのみを SAML 契約の IdP にインポートする必要があります。
- **ピア**：クラスタ内の各ピアに対してメタデータファイルを生成します。SAML 契約に対して、各メタデータファイルを IdP にインポートする必要があります。Expressway が以前の SAML SSO 対応リリースから 12.5 にアップグレードされると、[ピア（Peer）] オプションがデフォルトで選択されます。

新しい展開の場合、[SAMLメタデータ（SAML Metadata）] モードは常にデフォルトで**[クラスタ（Cluster）]** に設定されます。

既存の展開の場合、以前の Expressway リリースで SAML SSO が無効になっている場合、モードはデフォルトで **[クラスタ（Cluster）]** になり、SAML SSO が以前に有効になっている場合は **[ピア（Peer）]** になります。

ステップ 3 **[SAMLデータをエクスポート（Export SAML data）]** をクリックします。

このページには、接続された Expressway-E、またはクラスタの場合はすべての Expressway-E ピアが一覧されます。これは、これらのデータが、Expressway-C の SMAL メタデータに含まれるためです。

ステップ 4 SAML メタデータに **[クラスタ（Cluster）]** を選択した場合は、**[証明書の生成（Generate Certificate）]** をクリックします。

ステップ 5 次の手順を実行します。

- クラスタ全体のモードで、単一のクラスタ全体のメタデータファイルをダウンロードするには、**[ダウンロード（Download）]** をクリックします。
- ピアごとのモードで、個々のピアのメタデータファイルをダウンロードするには、ピアの横にある **[ダウンロード（Download）]** をクリックします。すべてを .zip ファイルにエクスポートするには、**[すべてダウンロード（Download All）]** をクリックします。

ステップ 6 生成されたファイルをコピーし、IdP に SAML メタデータをインポートする必要がある際にアクセスできる安全な場所にペーストします。

IdP から SAML メタデータをインポート

ステップ 1 Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[アイデンティティプロバイダー（IdP）（Identity providers (IdP)）]** の順に選択します。

これを実行する必要があるのは、クラスタのプライマリ ピアのみです。

ステップ 2 **[SAMLから新しいIdPをインポート（Import new IdP from SAML）]** をクリックします。

ステップ 3 **[SAMLファイルをインポート（Import SAML file）]** コントロールを使用して、IdP から SMAL メタデータファイルを検索します。

ステップ 4 **[ダイジェスト（Digest）]** を必要な SHA ハッシュアルゴリズムに設定します。

Expressway はクライアントが IdP に提示する SAML 認証要求の署名にこのダイジェストを使用します。署名アルゴリズムは、SAML 認証要求の署名を検証するために IdP で想定されているものと一致している必要があります。

ステップ 5 [アップロード（Upload）] をクリックします。

Expressway-C は、IdP の通信を認証し、IdP に対する SAML 通信を暗号化できます。

（注） メタデータをインポートした後は、**[（Configuration）]** > **[Unified Communications]** > **[アイデンティティプロバイダ（IdP）（Identity providers (IdP)）]** の順に選択し、IdP 行を検索し、アクション列で **[ダイジェストの構成（Configure Digest）]** をクリックすると署名アルゴリズムを変更できます。

IdP とドメインの関連付け

ドメインの MRA ユーザーを IdP を介して認証する場合は、IdP にそのドメインを関連付ける必要があります。少なくとも 1 つのドメインを関連付けるまで IdP は値を追加しません。

ドメインと IdP 間には多対 1 の関係があります。1 つの IdP を複数のドメインに使用できますが、各ドメインに関連付けられる IdP は 1 つだけです。

ステップ 1 Expressway-C で、IdP リストを開き（**[構成（Configuration）]** > **[Unified Communications]** > **[アイデンティティプロバイダー（IdP）（Identity providers (IdP)）]**）、IdP がリストにあることを確認します。

IdP はそのエンティティ ID 別に表示されます。それぞれ関連付けられたドメインが ID の横に表示されます。

ステップ 2 IdP の行で **[ドメインの関連付け（Associate domains）]** をクリックします。

これにより、Expressway-C のすべてのドメインが一覧されます。IdP にすでに関連付けられているドメインの横には、チェックマークが表示されます。また、リスト内の他のドメインに関連付けられている別の IdP がある場合は、IdP エンティティ ID も表示されます。

ステップ 3 この IdP に関連付けるドメインの横にあるチェックボックスをオンにします。

チェックボックスの横に、（転送）と表示されている場合、ドメインの既存の関連付けが解除され、この IdP にドメインが関連付けられます。

ステップ 4 [保存（Save）] をクリックします。

選択したドメインがこの IdP に関連付けられます。

SAML SSO に ADFS を構成

アイデンティティ プロバイダーに Active Directory フェデレーションサービス（ADFS）を使用している場合は、ADFS でこれらの追加構成を完了します。

Expressway-E の信頼当事者証明を作成後、各エンティティに一部のプロパティを設定し、Active Directory フェデレーションサービス（ADFS）が Expressway-E の期待通りに SAML 応答を作成することを確認します。また、各信頼当事者証明にクレームルールを追加する必要があります。

ステップ 1 応答全体に署名するよう ADFS を構成します。信頼当事者証明が ADFS で作成されたら、Windows PowerShell® で、各 Expressway-E <Name> に対して次のコマンドを実行します。

`Set-ADFSRelyingPartyTrust -TargetName "<Name>" -SAMLResponseSignature MessageAndAssertion`。<Name> は、ADFS で設定されている Expressway-E の 信頼当事者証明の名前に置き換えてください。

ステップ 2 各信頼当事者証明にクレームルールを追加する。

a) **[クレームルールの編集（Edit Claims Rule）]** ダイアログを開き、AD 属性にクレームとして送信される新規クレームルールを作成します。
b) 内部システムに対して OAuth ユーザーを識別するもの（通常は電子メールまたは SAMAccountName）に一致する AD 属性を選択します。
c) **[進行中のクレームタイプ（Outgoing Claim Type）]** として **`uid`** を入力します。

セキュアトラバーサルゾーンの構成

Expressway-C と Expressway-E の両方で、タイプ「Unified Communications traversal」の暗号化ゾーンを構成します。 Expressway-C と Expressway-E の両方で手順を完了します。

（注） この構成は、TLS検証モードはオンに設定され、メディア暗号化モードは[暗号化を強制（Force encrypted）]に設定された状態でSIP TLSを使用する適切なトラバーサルゾーン（Expressway-Cで選択した場合は、トラバーサルクライアントゾーン、Expressway-Eで選択した場合は、トラバーサルサーバーゾーン）を自動設定します。

始める前に

- Expressway-C と Expressway-E が互いの証明書を信頼していることを確認してください。各 Expressway がクライアントとサーバの両方として機能すると同時に各 Expressway の証明書がクライアントとサーバとして有効であることを確認する必要があります。証明書交換要件の詳細については、「証明書の要件」を参照してください。
- Expressway は、CN ではなく、SAN 属性を使用して受信した証明書を検証することに注意してください。
- H.323 または暗号化されていない接続も必要な場合、別のトラバーサル ゾーン ペアを設定する必要があります。

ステップ 1 Expressway-C プライマリプアで、**[構成（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]**の順に選択します。

ステップ 2 [新規（New）] をクリックします。

ステップ 3 以下の表のフィールドを構成します。適切な Expressway サーバー（C または E）の設定を適用します。

表 *2 : UC* トラバーサルゾーンの設定

フィールド	**Expressway-C の設定**	**Expressway-E の設定**
名前	「Traversal zone」など	「Traversal zone」など
タイプ（Type）	Unified Communications traversal	Unified Communications traversal
[接続クレデンシャル（Connection credentials）] セクション		
ユーザー名（Username）	「exampleauth」など	「exampleauth」など

フィールド	Expressway-C の設定	Expressway-E の設定
パスワード	「ex4mpl3.c0m」など	**[ローカル認証データベースの追加/編集（Add/Edit local authentication database）]** を選択します。ポップアップダイアログで、**[新規（New）]** をクリックし、**名前**（例：「exampleauth」）と**パスワード**（例：「ex4mpl3.c0m」）を入力し、**[ログイン情報を作成（Create credential）]** をクリックします。
SIP セクション		
ポート（Port）	Expressway-E の設定に一致する必要があります。	`7001`（デフォルト）『Cisco Expressway シリーズ設定ガイド』ページのご使用のバージョンの『*Cisco Expressway IP* ポート使用設定ガイド』を参照してください。
TLS サブジェクト名の確認（TLS verify subject name）	N/A	トラバーサルクライアントの証明書で、検索する名前を入力します（Subject Alternative Name 属性である必要があります）。トラバーサル クライアントのクラスタがある場合は、ここでクラスタ名を指定し、各クライアントの証明書に含まれることを確認します。
認証（Authentication） セクション		
[認証ポリシー（Authentication policy）]	[クレデンシャルを確認しない（Do not check credentials）]	[クレデンシャルを確認しない（Do not check credentials）]
ロケーション（Location） セクション		
ピア 1 アドレス（Peer 1 address）	Expressway-E の FQDN を入力します。 注：IP アドレスを使用する場合（推奨していません）、そのアドレスが Expressway-E サーバ証明書に含まれている必要があります。 MRA のデュアル NIC インターフェイスで Expressway-E を構成している場合は、Expressway-E の内部インターフェイスの FQDN を入力します（IP アドレスではありません）。Expressway-C には、Expressway-E の内部 LAN の FQDN を指すローカルドメインネームシステム（DNS）レコードが必要です。	N/A

フィールド	Expressway-C の設定	Expressway-E の設定
ピア 2 ～ 6 アドレス（Peer 2...6 address）	Expressway-E のクラスタである場合は、追加ピアの FQDN を入力します。	N/A

ステップ 4 [ゾーンの作成（Create zone）] をクリックします。

ステップ 5 Expressway-E プライマリピアでこれらの手順を繰り返し、Expressway-E 列の設定を適用します。

セキュア通信の構成

この展開には、Expressway-C と Expressway-E、および Expressway-E と企業外にあるエンドポイント間のセキュア通信が必要です。これには、HTTP、SIP、および XMPP の暗号化された TLS 通信の義務化、および該当する場合は証明書の交換とチェックが含まれます。Jabber エンドポイントは、Unified CM で保持されているログイン情報に対して検証される有効なユーザー名とパスワードの組み合わせを提供する必要があります。すべてのメディアが SRTP で保護されます。

Expressway-C は、Expressway-C と検出された各 Unified CM ノード間で構成できないネイバーゾーンを自動生成します。TCP ゾーンは常に作成されます。TLS ゾーンは、 Unified CM ノードが**クラスタセキュリティモード（[システム（System）] > [企業パラメータ（Enterprise Parameters）] > [セキュリティパラメータ（Security Parameters）]**）が *1*（混合）で構成されている場合に作成されます（これにより、セキュアなプロファイルでプロビジョニングされたデバイスがサポートされます）。TLS ゾーンは、Unified CM が TLS 検証モードを有効になっている場合、**[TLS検証モード（TLS verify mode）]** が *[オン（On）]* の状態で構成されます。これは、Expressway-C が後続の SIP 通信用の CallManager 証明書を確認することを意味します。

（注） Unified CM が混合モードでない場合、セキュアプロファイルは TCP を使用するようにダウングレードされます。

Unified CM パブリッシャ が Expressway に追加（または更新）された場合、Unified CM への Expressway ネイバーゾーンは、Unified CM が返す Unified CM ノードの名前を使用します。Expressway は、これらの返された名前を使用して Unified CM ノードに接続します。その名前がホスト名だけの場合

- その名前を使用してルーティング可能である必要があります
- これは、Expressway が Unified CM のサーバー証明書に公開されることを想定する名前です

セキュア プロファイルを使用している場合、 Expressway-C の証明書に署名した認証局のルート CA が CallManager の信頼証明書（Cisco Unified OS の管理アプリケーションの**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**）としてインストールされていることを確認します。

メディア暗号化

メディア暗号化は Expressway-C と Expressway-E 間、および企業外にある Expressway-E とエンドポイント間のコールレッグで実行されます。

暗号化は、メディアが Expressway-C の B2BUA にパススルーするときに物理的に適用されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。